47. A device according to Claim 46 wherein a column shift operation performed by each of said plurality of shift column modules generates shift column data, and wherein said circuit further comprises a single mix column module to perform column mix operations on shift column data.

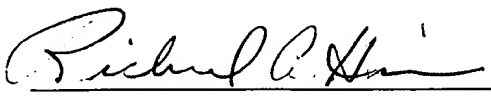
REMARKS

For better readability and the Examiner's convenience, the newly submitted claims differ from the translated counterpart claims, which are being canceled. The newly submitted claims do not represent changes or amendments that narrow the claim scope for any reason related to the statutory requirements for patentability.

It is believed that all of the claims are patentable over the prior art. Accordingly, after the Examiner completes a thorough examination and finds the claims patentable, a Notice of Allowance is respectfully requested in due course. Should the Examiner determine any minor informalities that

need to be addressed, he is encouraged to contact the undersigned attorney at the telephone number below.

Respectfully submitted,



RICHARD A. HINSON
Reg. No. 47,652
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330
Attorneys for Applicants

In re Patent Application of:
MACCHETTI ET AL.
Serial No. **09/974,705**
Filed: **October 10, 2001**

_____/

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In the specification:

The heading -- Background of the Invention - has been inserted at line 9 of page 1 immediately before the paragraph beginning there, and the paragraph has been amended to read as follows:

--The Rijndael algorithm is a block cipher algorithm operating on blocks of data. The algorithm reads an entire block of data, processes the block and then outputs the encrypted data. The Rijndael algorithm needs a key, which is another block of data. The proposed AES standard will include [only] a 128-bit standard length for plaintext blocks and 128, 192 and 256-bit [as] standard lengths for the key material.--

The heading "Description of the prior art" has been deleted at line 17 of page 1.

The paragraph beginning at line 20 of page 4 has been amended as follows:

-- In the diagram of figure 4, reference numeral 12 designates a [demux unit] demultiplexer which distributes the input unencrypted data stream UD over four different paths leading to respective adder modules 14a, 14b, 14c and 14d where the first key addition is performed. --

The paragraph beginning at line 25 of page 4 has been amended as follows:

--Reference numerals 24a, 24b, 24c and 24d designates respective sets of byte [register] registers wherein the 32-bit words subjected to the first key addition are distributed over four byte registers to be subsequently fed to respective sets of modules 34a, 34b, 34c and 34d where the S-box processing takes place.--

The paragraph beginning at line 21 of page 5 has been amended as follows:

--The main disadvantage of the prior art solutions exemplified by the arrangement shown in figure 4 lies in the complex circuitry required to implement the encryption/decryption mechanism. Such a disadvantage is particularly felt to those envisaged applications of cryptosystems adapted for use in embedded systems such as, e.g., smartcards and the like.—

The heading -Summary of the Invention- has been inserted at line 28 of page 5 immediately before the paragraph beginning there.

The paragraph beginning at line 32 of page 5 has been amended as follows:

--According to the present invention, this object, as well as additional objects [which will become apparent from the following detailed description of a preferred embodiment of the invention,] are achieved by means of a method and

system [having the features set forth in the annexed claims] using a transposed arrangement for the internal state array of a matrix to provide a more rapid encryption/decryption process. The present invention also provides a circuit for implementing the process.

The paragraph beginning at line 9 of page 6 has been amended as follows:

--The invention will now be described, by a way of non limiting example, by referring to the enclosed drawings, wherein:

-Figures 1 to 4, [exemplary of] illustrate prior art approaches for implementing the Rijndael/AES algorithm [have been already described in the foregoing],

-Figure 5 [is intended to highlight,] illustrates comparison to figure 3, the basic underlying mechanism of the present invention, and

-Figure 6 [shows how the system shown in the block diagram of figure 4 is modified and simplified by resorting] is a schematic diagram of a data encryption/decryption circuit according to the present invention.

The heading beginning at line 21 of page 6 has been amended as follows:

--Detailed Description of [a] the Preferred [embodiment] Embodiments of the Present Invention--

In re Patent Application of:
MACCHETTI ET AL.
Serial No. **09/974,705**
Filed: **October 10, 2001**
_____/

The paragraph beginning at line 23 of page 6 has been amended as follows:

--In order to better understand the basic underlying principle of the invention, it must be recalled that Rijndael is a secret key cryptographic algorithm working in block cipher mode. This means that it operates on blocks of data and not on single bits or bytes. The algorithm reads an entire block, processes it and then [output] outputs the encrypted block. The [encryption] decryption operates in a complementary way to re-obtain plaintext starting from [a] encrypted data.--

The paragraph beginning at line 6 of page 7 has been amended as follows:

--The following description will therefore deal - by way of example only - with 128-bit blocks, as this adheres to the presently [prospected] prognosticated standard.--

The paragraph beginning at line 34 of page 8 has been amended as follows:

--Transposed Form $x_i = S_{0,i}\ S_{1,i}\ S_{2,i}\ S_{3,i}$

where x_i, $0 \leq i \leq 3$ are the words of the transposed state, and y_i, $0 \leq i \leq 3$ are the words of the transposed state after mix column transformation.--

The paragraph beginning at line 10 of page 9 has been amended as follows:

--Such a transposition requires a redefinition of [must] most of the operations performed in a round of the algorithm, and also if the key schedule. Therefore, also the round keys must be transposed before being applied to a round providing for the use of a transposed state.--

The paragraph beginning at line 23 of page 9 has been amended as follows:

--This means that the internal [behaviour] behavior of the system is modified, and simplified, the only requirement to obtain compatibility with the standard being that the state must be re-transposed before being [output] outputs.--

In the Abstract:

The title of the abstract beginning at line 1 of page 15 has been amended as follows:

--Abstract of the Disclosure—

The paragraph beginning at line 2 of page 15 has been amended as follows:

--Data are converted between an unencrypted and an encrypted format according to the Rijndael algorithm, including a plurality of rounds. Each round is comprised of a fixed set of transformations applied to a two-dimensional array, [designated state] designating states, of rows and columns of bit words. At least a part of [said] the transformations are applied on a transposed version of the state, wherein rows and columns are transposed for the columns and rows, respectively.

[(Figure 6)]--

In re Patent Application of:
MACCHETTI ET AL.
Serial No. **09/974,705**
Filed: **October 10, 2001**
_____/

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: DIRECTOR, U.S. PATENT AND TRADEMARK OFFICE, WASHINGTON, D.C. 20231, on this 8th day of April, 2002.

Kevin L. Patron